# DECLARATION OF GUY GINO

I, Guy Gino, do hereby declare:

## AGENT BACKGROUND AND TRAINING

1. I am a Special Agent (SA) with Homeland Security Investigations (HSI) and have been so employed since 2003. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7) and I am authorized by law to conduct investigations and to make arrests for felony offenses. I am currently assigned to the Assistant Special Agent in Charge of HSI, Portland, Oregon. Prior to this, I was employed as a U.S. Border Patrol Agent and have been a federal law enforcement officer since September 1996. During my tenure as a federal law enforcement officer, I have investigated and/or participated in investigations of conspiracy, money laundering, narcotics trafficking, fraud, smuggling and theft. I have also acquired knowledge and information about the illegal drug trade and the various means and methods by which it is furthered, including through the use of computers, smart phones, digital media and the Internet, from formal and informal training, other law enforcement officers and investigators, informants, individuals I have arrested and/or interviewed, and from my participation in other investigations.

2. I am a Subject Matter Expert on the tracing of and use of cryptocurrency as part of money laundering schemes utilized by criminals to launder their illicit proceeds. As part of this area of expertise, I have created and conducted training on the use of and how to trace cryptocurrency to dozens of domestic and foreign law enforcement agencies since 2015. I have also provided expert testimony in trials regarding the illicit use of and the tracing of cryptocurrency in three occasions in the Districts of Utah, New Jersey and the Western District of Tennessee.

**PURPOSE OF DECLARATION**

3. This declaration is submitted in support of a complaint for forfeiture. The information contained in this declaration is based on an investigation I conducted, which will show that $187,182.67 in U.S. currency—which represents converted cryptocurrency obtained from SHAISHAV RAMAVAT's OKX Exchange Account # 301953210925592576—was involved in transactions or attempted transactions or traceable to money laundering offenses in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1957 (unlawful monetary transactions in excess of $10,000), and is property constituting or derived from proceeds obtained, directly or indirectly, from a violation of 18 U.S.C. § 1343 (wire fraud). These funds are subject to seizure pursuant to 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C).

4. The facts set forth in this declaration are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. This declaration does not set forth each and every fact that I or others have learned during the course of this investigation, only those necessary to establish probable cause to believe the currency is now subject to seizure pursuant to 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C).

## SUMMARY OF INVESTIGATION

5. Homeland Security Investigations is investigating a fraud scheme conducted by a Transnational Criminal Organization in which the perpetrators trick and coerce their victims—some who are elderly—into providing them money in the form of bitcoin. All the victims detailed below fell prey to a scheme that involved messages designed to create a sense of urgency. This was accomplished by telling victims that they have some sort of serious legal problem and that if they did not immediately take a particular action demanded by the callers then there would be drastic consequences, specifically involving the arrest of the victims and/or significant financial penalties. The fraudsters instructed the victims that in order to prevent these dire consequences, the victims must pay money using the cryptocurrency bitcoin to some supposed government entity.

## STATEMENT OF PROBABLE CAUSE

**Oregon Investigation – Victim 1**

6. On September 6, 2022, Deschutes County Sheriff's Office initiated an investigation regarding a theft by deception after a 69-year-old resident of Bend, Oregon (hereafter identified as Victim 1) reported that they fell victim to a fraud scheme which resulted in the loss of approximately $23,991. The facts regarding that incident are as follows:

7. On September 6, 2022, Victim 1 received a telephone call from an unknown male claiming to be from Amazon. The male told the Victim 1 that they located several fraudulent purchases of Apple products using Victim 1's Amazon account and that the debt has not been paid. The call was then transferred from the unknown male at Amazon to an unknown female claiming to be with the U.S. Treasury Department. The unknown female told Victim 1 that if Victim 1 did not pay the debt, they (U.S. Treasury) would issue a warrant for Victim 1's arrest.

8. As Victim 1 travelled to their financial institution, the unknown female remained on the phone with Victim 1, inquired how much money Victim 1 had in their account, and instructed Victim 1 to withdraw the full contents of their bank account (which was approximately $24,000) in cash. The unknown female then instructed Victim 1 to go to a BitStop bitcoin kiosk at an address located in Bend, Oregon. The unknown female verbally told Victim 1 where to go.

9. At the BitStop bitcoin kiosk, Victim 1 started depositing the cash into the machine but was only able to deposit $9,900 before reaching the machine deposit limit. The female remained on the phone with Victim 1 and informed Victim 1 that another "U.S. Treasury official" would send Victim 1 the bitcoin address to send the bitcoin. Victim 1 received a QR code via SMS message instructing the bitcoin to be sent to bitcoin address bc1ql******9ceck. Victim 1 sent 0.44086281 bitcoin (BTC) to the designated address, as instructed.

10. Victim 1 was then instructed to go to a different bitcoin kiosk to deposit the remaining funds. Again, the unknown female remained on the phone with Victim 1 and verbally provided the location of the bitcoin kiosk and gave instructions to Victim 1 on where to send the bitcoin. Victim 1 deposited $13,210.00 into a CoinCloud bitcoin kiosk. Victim 1 entered the receiving address of bc1q3*****x86rn and completed the transaction by sending 0.57588463 BTC to the receiving address.

11. The caller remained on the phone with Victim 1 throughout the whole process. The call dropped twice which resulted in the purported U.S. Treasury official calling Victim 1 back to further provide instruction on sending the funds.

12. After Victim 1 realized they were possibly scammed they contacted the Deschutes County Sheriff's Office (DCSO) who opened an investigation.

13. On October 24, 2022, I was contacted by DCSO Sergeant Thomas Lilienthal who asked for my assistance in this investigation. Sgt. Lilienthal provided me with the initial report taken from Victim 1 and photographs of the two bitcoin kiosk receipts Victim 1 retained.

**Tracing of Victim 1's Bitcoin Transactions**

14. On October 25, 2022, I reviewed the two receipts Victim 1 provided and located the two confirmed transactions on the Bitcoin blockchain, which is the Bitcoin network's transparent public ledger, using a publicly available Bitcoin blockchain explorer. I know from my training and experience all confirmed transactions are posted and broadcasted on the blockchain upon confirmation.

15. Using the blockchain explorer, I observed Victim 1's first transaction, which they conducted on September 6, 2022, at 5:13 p.m. PDT, using the BTC Kiosk operated by BitStop in Bend, Oregon (hereafter referenced as ORTX1). This transaction involved the transfer of 0.44086281 BTC to bc1ql******9ceck.

16. By using the blockchain explorer, I was able to see all transaction history for address bc1ql******9ceck and noted that it had only received one deposit transaction (Victim 1's bitcoin transfer as part of ORTX1) and one withdrawal transaction, transferring 0.44084949 BTC to address 36rpd*****6VF8M.

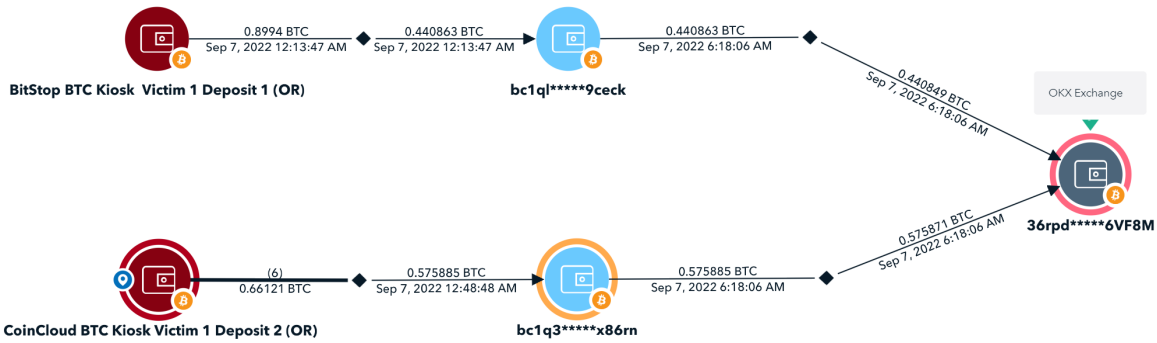
17. I applied the same methods as previously referenced and identified Victim 1's second transaction, which they conducted using a BTC Kiosk operated by CoinCloud in Bend, Oregon (hereafter referenced as ORTX2). I noted that this transaction occurred on September 6, 2022, at 5:48 p.m. PDT and involved the transfer of 0.57588463 BTC to address bc1q3*****x86rn.

18. Using the blockchain explorer, I was able to see all transactions in and out of bitcoin address bc1q3*****x86rn and noted that address only had one deposit transaction, which was part of ORTX2. The withdrawal transaction was part of TXID: c1612*****46a18 and involved a transfer of 0.57587131 BTC to 36rpd*****6VF8M, which I recognized as the same address that received Victim 1's funds from ORTX1.

19. I used a blockchain forensic tool, which identified that the transfer of the bitcoin from TXIDs: f5fc6*****df294 and c1612*****46a18 were both sent to an address owned by the OKX Exchange. I know that OKX is a cryptocurrency exchange headquartered and based in the Seychelles.

20. On October 25, 2022, I sent an email requesting information regarding TXIDs: f5fc6*****df294 and c1612*****46a18 to the OKX legal team.

21. On October 31, 2022, I received a voluntary response from OKX that included account information for user ID 301953210925592576. These records revealed the account was assigned to Shaishav RAMAVAT (hereafter referenced as RAMAVAT Account) and was created on April 18, 2022. The records included subscriber information for the account holder, email account, log in IP records, user operation log, user activity, and transaction logs. As part of this return, I was able to identify that RAMAVAT was assigned bitcoin address 36rpd*****6VF8M (hereafter referenced as VF8M Address). The below graph depicts the flow of bitcoin from Victim 1's deposits to the VF8M Address.




**Virginia Investigation – Victim 2**

22. On November 18, 2022, I was made aware of a separate investigation being conducted by Federal Bureau of Investigations (FBI) Special Agent Michael McGillicuddy of the FBI's Washington Field Office. In speaking with SA McGillicuddy, I was informed that his investigation identified two victims, hereafter referenced as Victim 2 and Victim 3, who were also subjected to a fraud scheme resulting in both victims sending bitcoin to addresses which then were subsequently sent to an address assigned to the RAMAVAT Account.

23. On or around September 26, 2022, Victim 2, residing in Newport News, Virginia, got a telephone call purportedly from "Amazon" saying that her bank account had been hacked. Victim 2 was then connected to an unidentified individual who, according to Victim 2's caller ID, was from "Bayport Federal Credit Union." This individual told her that her social security account number had been compromised. Finally, Victim 2 was forwarded to an individual identifying himself as "Mark Watson," purportedly from the "Federal Trade Commission," who advised her that there was money laundering and theft attached to her social security account number. Victim 2 was told that if she did not cooperate, she would be held accountable for the criminal conduct.

Victim 2 was advised that she needed to withdraw all but $500 from her checking account and all but $500 from her savings. At the caller's direction, Victim 2 proceeded to her nearest credit union location and withdrew $4,900 in cash. Watson then told Victim 2 to go to a specific supermarket in Newport News and to deposit the cash into a bitcoin kiosk, which would hold Victim's 2 money until Victim 2 received a new social security account number. Victim 2 did as Watson instructed and subsequently sent a screenshot of the deposit to Watson, as well as a screenshot of the kiosk's text confirmation. At that point, the banks were closed, so Victim 2 was advised to await Watson's call the following morning.

24. On or around September 27, 2022, again at Watson's direction, Victim 2 left work to withdraw $16,970 in cash from a larger credit union location. Victim 2 then went back to the same supermarket, deposited the cash into the bitcoin kiosk, and sent the screenshots. Victim 2 eventually returned to work but was directed to keep their phone connected to Watson and in their bag the entire time. Watson then told Victim 2 that Victim 2's credit cards had also been compromised and Victim 2 had to withdrawal all the available money on the cards to avoid bankruptcy. Only one of Victim 2's credit cards had an actual bank branch (Bank of America) in Victim 2's vicinity. As a result, Victim 2 again left work, took out a $3,600 cash advance on the credit card, drove back to the same supermarket, deposited the cash into the bitcoin kiosk, and forwarded the screenshots. Later that same evening, Victim 2 researched their situation and found out that it was a scam. As a result, Victim 2 immediately filed a complaint with both the Newport News Police Department and the FBI's Internet Crime Complaint Center ("IC3") for a total reported loss of $25,470.

25. On or around September 30, 2022, at SA McGillicuddy's request, Victim 2 provided him with the above-referenced screenshots of the text confirmations of their three bitcoin kiosk deposits. SA McGillicuddy reviewed those confirmations using a publicly available bitcoin blockchain explorer. SA McGillicuddy informed me that collectively, they indicated that Victim 2's above-referenced cash deposits resulted in 1.070434 BTC being deposited into bitcoin address 3Flub*****VEMYT at a bitcoin kiosk operated by ByteFederal.

**Tracing of Victim 2's Bitcoin Transactions**

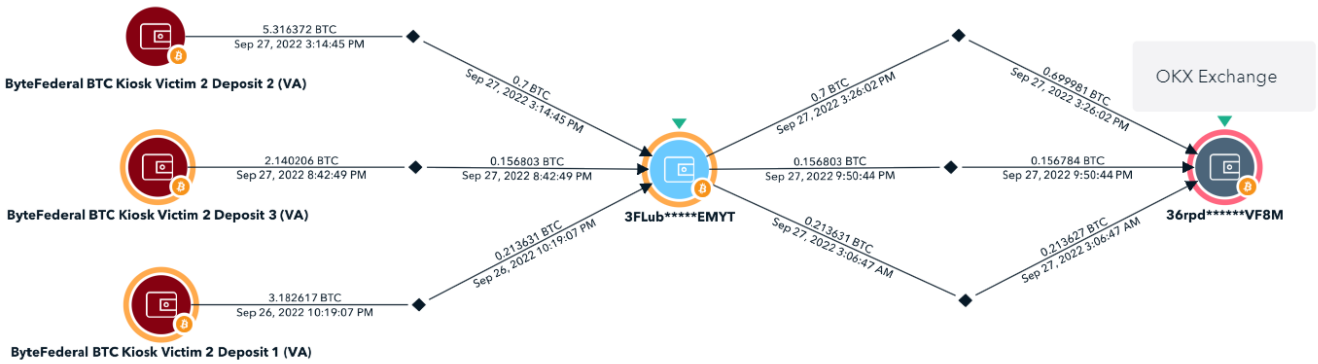
26. I reviewed the screenshots provided to SA McGillicuddy by Victim 2. Using the publicly available bitcoin blockchain explorer, I observed Victim 2's three transactions. The first transaction (hereafter referenced as VATX1)—which they conducted using the bitcoin kiosk operated by ByteFederal in Newport News, Virginia—occurred on September 26, 2022, at 11:19 a.m. EDT and involved the transfer of 0.213631 BTC to address 3Flub*****EMYT.

27. Using the blockchain explorer, I was able to see the transactions history for bitcoin address 3Flub*****EMYT and noted that on that same day, prior to VATX1, the address had received four separate deposits followed by three withdrawals. I noted that after each deposit into 3Flub*****EMYT, there would be a subsequent withdrawal within an hour that would empty the funds from 3Flub*****EMYT. This pattern of activity didn't change after 3Flub*****EMYT received the deposit from VATX1. I observed that after receiving this deposit, the next transaction transferred to 0.213627 BTC to the VF8M Address.

28. During my review of bitcoin address 3Flub*****EMYT transactions, I was able to identify the two subsequent transactions that occurred after VATX1. I observed that on September 27, 2022, at 11:14 a.m. EDT, 3Flub*****EMYT received a transfer for 0.7 BTC (VATX2). I noted

that after the 0.7 BTC was received, it remained at the address for twelve minutes until being transferred to the VF8M Address.

29. The next inbound transaction into 3Flub*****EMYT, consistent with Victim 2's third bitcoin kiosk deposit, occurred on September 27, 2022, at 4:42 p.m. EDT, when the address received 0.156803 BTC. Again, after receipt of the bitcoin and within eight minutes, the 0.156803 was transferred to the VF8M Address. The below graph depicts the flow of bitcoin from Victim 2's deposits to the VF8M Address.




**Alabama Investigation – Victim 3**

30. On October 19, 2022, as part of his investigation into the individual or individuals responsible for the fraud scheme involving Victim 2, SA McGillicuddy learned about another fraud involving the above-referenced VF8M Address. SA McGillicuddy interviewed Victim 3, residing in Wetumpka, Alabama, who advised that they were a victim of a scam. Specifically, on or around July 29, 2022, Victim 3 received a telephone call from an individual identifying himself as "Bruce Jennings," purportedly from the "Federal Trade Commission." At Jennings's direction, on July 29

and July 30, 2022, Victim 3 deposited $16,000 and $8,500 in cash, respectively, into a CoinFlip kiosk. As of January 10, 2023, Victim 3 had not recovered any of the $24,500 they deposited.

31. SA McGillicuddy told me that he reviewed Victim 3's deposits using a publicly available bitcoin blockchain explorer and observed Victim 3's transfers. Both of Victim 3's deposits (minus small associated fees) were transferred to the VF8M Address within two hours of being received. Specifically, less fees, a total of 0.88498123 BTC was transferred to the VF8M Address on July 29 and July 30, 2022.

32. On January 20, 2023, SA McGillicuddy provided me with his report covering his interview of Victim 3 and other investigative materials so that I could conduct my own analysis.

**Tracing of Victim 3's Bitcoin Transactions**

33. I reviewed SA McGillicuddy's interview of Victim 3 and other investigative materials.

34. I used the blockchain explorer to analyze each transaction. I observed that ALTX1 occurred on July 29, 2022, 2:39 p.m. CDT and, as part of that transaction, 0.583407 BTC was received by address 38Rrd*****QA7Hf.

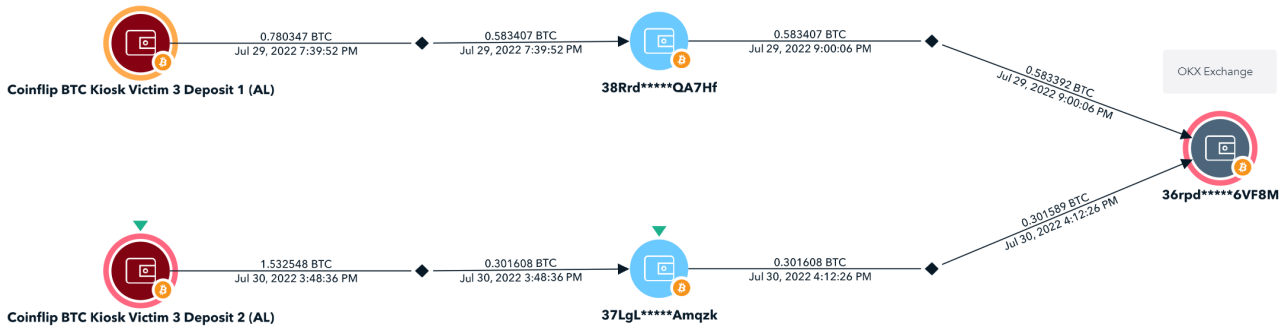
35. Using the blockchain explorer, I was able to see all transaction history for address 38Rrd*****QA7Hf and noted that on that same day, prior to receiving ALTX1, it had two separate inbound transfers of bitcoin that were followed by two outbound transactions occurring within minutes of being received. I noted that for each instance when 38Rrd*****QA7Hf received bitcoin, it would transfer the bitcoin to the VF8M Address. I also recognized that after each subsequent outbound transaction, 38Rrd*****QA7Hf would be left with a zero balance. I observed similar

activity after 38Rrd*****QA7Hf received ALTX1 from Victim 3. Approximately twenty-one minutes after receipt, the 0.583406 BTC was transferred to the VF8M Address.

36. Using the blockchain explorer, I observed that ALTX2 occurred on July 30, 2022, 10:48 a.m. CDT, and as part of that transaction 0.301608 BTC was transferred to address 37LgL*****Amqzk. I noted that after the 0.301608 BTC was received, it was transferred twenty-five minutes later to the VF8M Address.

37. I reviewed the transaction history of address 37LgL*****Amqzk and learned that prior to ALTX2 there were no other inbound transactions.

38. The below graph depicts the flow of bitcoin from Victim 3's deposits to the VF8M Address.




**California Investigation – Victim 4**

39. On January 27, 2023, I was made aware of a separate investigation being conducted by Federal Bureau of Investigations (FBI) Special Agent Brian Myers of the FBI's Sacramento Field Office. In speaking with SA Myers, I was informed that his investigation identified a victim, hereafter referenced as Victim 4, who was also subjected to a fraud scheme in which he was tricked

and coerced into sending bitcoin to multiple addresses which were subsequently sent to the RAMAVAT Account.

40. On August 5, 2022, Victim 4, residing in Visalia, California, received a phone call from an unknown individual claiming to be from Amazon who informed Victim 4 of fraudulent activity on his account. The unknown individual forwarded Victim 4 to an unknown male claiming to be a Chase Bank representative. The unknown male said that unknown subjects have been using Victim 4's medical doctor identification and conducting fraudulent activities. The unknown male told Victim 4 that he was going to transfer him to the Federal Trade Commission (FTC) who were going to help secure Victim 4's various bank accounts. Victim 4 was subsequently transferred to another unknown male subject claiming to be "Alex Watson" from the FTC. Watson told Victim 4 that their identity had been stolen and the FTC needed to freeze their bank accounts. Watson convinced Victim 4 that they could "safeguard" their accounts if Victim 4 deposited cash from their accounts to a bitcoin ATM and transferred the funds to a bitcoin address provided by Watson. Watson told Victim 4 to keep this secret and to not inform anyone of the stolen identity or of the deposits. Watson convinced Victim 4 they would receive all the funds back via a check.

41. On September 26, 2022, Victim 4 received a text message from Watson which stated, "Sorry to scam you, Regards Alex Watson". Upon receipt of this message Victim 4 contacted the FBI in Bakersfield, California.

42. The following day Victim 4 met with FBI SA Myers and was interviewed. Victim 4 provided screenshots of text messages from Watson as well photographs of receipts from each bitcoin kiosk deposit. By reviewing the receipts, SA Myers was able to determine that between the period of August 5, 2022, through September 1, 2022, Victim 4 sent twenty-one transfers that

cumulatively totaled 9.33418507 BTC, valued at approximately $257,416, based on the U.S. dollar value at the time of each transaction.

43. On February 3, 2023, SA Myers provided me with the screenshots and photographs of the receipts he received from Victim 4 so I could conduct my own analysis of those transactions.

**Tracing of Victim 4's Bitcoin Transactions**

44. I reviewed the Victim 4 documentation provided to me by SA Myers and was able to ascertain that of the twenty-one transactions, eleven transactions cumulatively totaling 4.80785286 BTC were sent to intermediary wallet addresses, which shortly thereafter were sent to the VF8M Address.

45. For these eleven transactions, consistent with the other victims, Victim 4 deposited cash into bitcoin kiosks, including CoinCloud, CoinFlip, and Bitcoin Depot. When Victim 4 transferred the bitcoin to the Watson-provided address, each destination address had very few or no prior transactions. Any prior transactions were largely consistent with being other fraud scheme transactions. Also consistent with the other victims, shortly after Victim 4 transferred the bitcoin, the perpetrator transferred the funds out of the account, ultimately ending up in the VF8M Address.

**Analysis of Shaishav RAMAVAT's OKX Account**

46. As I previously mentioned, on October 31, 2022, I received a voluntary response from OKX that identified the VF8M Address as part of an account assigned to Shaishav RAMAVAT, an Indian citizen who resides in the Republic of India.

47. On February 3, 2022, I also received an updated version of those records from SA Myers, who as part of his investigation received the records from OKX voluntarily.

48. I reviewed the returned information regarding the RAMAVAT Account. I noted that RAMAVAT created the account on April 18, 2022, who, as part of his account creation process, provided a selfie picture and a copy of his Election Commission of India Identity Card, which contained his photograph. I identified that the account was authorized to conduct peer to peer (P2P) trading[1] with other OKX users on their P2P Marketplace.

49. I reviewed the RAMAVAT Account's transaction history and as part of my review I was able to ascertain that there was one deposit and one withdrawal on April 19, 2022 (the day after the account opened), but no transactions between April 19 and July 13, 2022. However, I noted for the period of July 14, 2022, through October 10, 2022, the RAMAVAT Account received 188 bitcoin deposits into the VF8M Address totaling 64.39406 BTC or approximately $1,351,121 (this total is based on the value of bitcoin at the time of each transaction into the RAMAVAT Account).

50. During my review of these records, I was able to locate the transactions I highlighted earlier involving a total of 7.78002 bitcoin Victims 1–4 sent that ultimately went to the RAMAVAT Account.

51. Furthermore, I was able to identify that once the RAMAVAT Account received these transactions, RAMAVAT used the exchange's P2P Marketplace to convert the cryptocurrency from bitcoin to Tether (USDT) and at times vice versa. Tether (USDT) is another

1 According to OKX webpage "P2P Trading is a peer-to-peer marketplace which allows users to buy and sell digital assets, such as Bitcoin, Tether and other cryptocurrencies, directly between users." OKX does not conduct trades on behalf of its users, rather, OKX operates as an escrow to ensure a fair trading experience.

type of cryptocurrency called a stablecoin.[2] These conversions or trades occurred usually within hours of deposit of the bitcoin into the RAMAVAT Account.

52. During my review, I identified the RAMAVAT Account had fifty-five USDT outbound transfers to ten external wallet addresses totaling 1,334,934.3750 USDT ($1,334,934.38).

53. I also observed that between August 8, 2022, through October 3, 2022, the RAMAVAT Account received nineteen USDT deposits from external accounts, which cumulatively totaled 231,134 USDT ($231,134). Some of these deposits originated from wallet addresses that had also received Tether from the RAMAVAT Account. When the RAMAVAT Account would receive an external Tether deposit, the RAMAVAT Account would rapidly send the same quantity of Tether to a different address. Based on my training and experience, I believe this behavior does not serve any legitimate business or investment purpose.

54. I know from my training and experience that criminals will often attempt to "clean" proceeds of illicit activity they receive in one form of cryptocurrency by converting them to a different form of cryptocurrency to hide the true source of those funds. Due to the transparent nature of the blockchain and the fact that bitcoin transactions are pseudonymous and can be traced, criminals will seek to immediately convert them into a different asset using an exchanger. This technique is referred to as "chain hopping" and represents moving funds from one blockchain to another in a manner to attempt to hide the transactional trail.

55. I also know from my training and experience that it is common practice for criminals to transfer their converted cryptocurrencies through multiple exchanges to further clean their

2 A stablecoin is a cryptocurrency for which the issuer attempts to have the value of the coin directly track its corresponding fiat currency, in this case the U.S. dollar.

transactional path. Based on my review of the transaction records, I believe the RAMAVAT Account is being utilized in this fashion.

56. Utilizing a forensic blockchain forensic tool, I conducted an analysis of the 190 bitcoin deposits received by the RAMAVAT Account. I learned that 89.84% or $1,213,804,[3] originated from bitcoin kiosks. I was able to identify all bitcoin kiosk operators that facilitated the transactions, and the percentage of quantities received by the RAMAVAT Account. The bitcoin kiosk operators and their percentages are as follows:

Athena Bitcoin 2.2%

Coinhub.com 3.43%

Bitcoin of America 15.21%

Rocketcoin ATM 16.28%

CoinCloudATM.com 17.80%

BitcoinDepot.com 22.09%

Coinflip.com 20.02%

57. I was able to identify that these bitcoin kiosk operators, with exception of Athena Bitcoin and CoinFlip, only operate within the United States. I know that Athena Bitcoin and CoinFlip operate kiosks both inside and outside of the United States.

58. Based on my training and experience, I believe the high volume of deposits into the RAMAVAT Account originating from bitcoin kiosks indicate that these funds are likely criminal proceeds. Each of the Victims 1–4 was instructed to deposit cash into bitcoin kiosks of various

3 This calculation is based on the value of bitcoin at the time of each transaction.

companies, which shows that this is the preferred method of the criminal organization to obtain criminal proceeds.

59. OKX informed me that at the time of their response, the RAMAVAT Account contained approximately 5.68443 BTC and 28,949.57 USDT. Although the cryptocurrency traceable to Victims 1–4 has been transferred out of the RAMAVAT Account, based on the continued activity of the account consistent with the fraud scheme and my analysis detailed below, I believe the cryptocurrency that was held in the account at that time is also proceeds of criminal activity.

**Analysis of Defendant Property**

60. During my review, I observed that at the end of September 15, 2022, the RAMAVAT Account's balance contained 0.0005902 BTC and 0.693251284086599973 USDT. At that time, these quantities were valued at approximately $81.00.

61. Between the period of September 16, 2022, through September 27, 2022, I observed the same pattern of daily activity consistent with the RAMAVAT Account since July 28, 2022. Specifically, 12.37075 bitcoin were deposited into the VF8M Wallet via multiple transactions, I was able to ascertain via tracing that the bitcoin was from deposits into U.S.-based bitcoin kiosks. I therefore believe these deposits represent bitcoin belonging to other unknown victims of this fraud scheme. These deposits were followed by almost immediate conversion into Tether on the OKX P2P Marketplace. I observed that the RAMAVAT Account made two withdrawals during this period totaling 0.075165 bitcoin ($1,488) to an account I was able to identify as RAMAVAT's Binance Account.

62. On September 27, 2022, the RAMAVAT Account's balance consisted of 0.00363173 BTC and 195,023.60043 USDT.

63. From September 28 to October 3, 2022, I observed fewer bitcoin deposits and much more activity indicative of money laundering and attempts to obfuscate the ownership and origination of the cryptocurrency.

64. On September 28, 2022, during the first ten hours of activity, I observed a transfer of 10,000 USDT to an external wallet address TJdzi*****uRFaj (hereafter referenced as RFaj Address) which is hosted by the Binance exchange and is assigned to an individual residing in India. This transfer out is followed by four deposits of bitcoin into the VF8M Address and the usual conversion into Tether. The four bitcoin deposits, totaling 0.365972 BTC, consisted of two transfers originating from U.S.-based bitcoin kiosks and two from the U.S.-based cryptocurrency exchange Kraken.

65. I observed that nine hours later, the account received two external Tether deposits of 7,322.96 USDT and 23,000 USDT totaling 30,322.9656 USDT into the RAMAVAT Account's Tether wallet. The 7,322.96 USDT originated from a ByBit exchange USDT wallet address and the 23,000 USDT originated from the unhosted USDT wallet address TE6HM*****FrcRA (hereafter referenced as rcRA Address).

66. At this time, I observed RAMAVAT Account activity that was out of character with what I have previously observed during the RAMAVAT Account's lifetime. The RAMAVAT Account converted 200,000 USDT—which it had accumulated in its funding wallet and represented converted bitcoin originating from U.S. based bitcoin deposits—to 10 bitcoin. In three transactions,

the account sent 5 bitcoin to an external unhosted bitcoin wallet address.[4] I also observed that the RAMAVAT Account transferred 20,000 USDT to the RFaj Address (as described above had previously received 10,000 USDT hours earlier). At the end of the day, the RAMAVAT Account had a new balance of 5.49178 BTC and 12,628.053679 USDT.

67. On September 29, 2022, the RAMAVAT Account received 19,500 USDT from USDT Address 8By3i******JFar6 (hereafter referenced as Far6 Address), which is hosted by the Binance exchange and is assigned to an individual residing in India. The account did not receive any bitcoin deposits but resumed using the P2P Marketplace to convert bitcoin into Tether. At the end of the day, the RAMAVAT Account balance contained 5.49058 BTC and 32,236.424767 USDT.

68. On September 30, 2022, the VF8M Address received 0.39952 BTC originated from a bitcoin kiosk. The RAMAVAT Account continued using the P2P Marketplace to convert bitcoin into Tether. After conversion to Tether, the RAMAVAT Account sent 8,709 USDT to an external unhosted wallet address. The RAMAVAT Account also received 21,200 USDT from two transfers, 20,000 USDT from the Far6 Address (that had sent 19,500 USDT to the RAMAVAT Account the previous day) and 1,200 USDT from an unhosted external wallet address. Within 3 hours of receiving the 20,000 USDT from the Fra6 Address, the RAMAVAT Account transferred 20,000 USDT to the RFaj Address. After the day's transactions, the new balance for the RAMAVAT Account consisted of 5.50186 BTC and 12,510 25111 USDT.

---

4 Unless specifically referenced, the identity of these wallet addresses is not relevant to the tracing analysis and therefore are not identified in this affidavit and do not recur in the tracing analysis. Therefore, each unidentified wallet should be considered separate wallet addresses.

69. In summary, on September 28, 20,000 USDT went from RAMAVAT Account to the RFaj Address followed the next day by a 19,500 USDT deposit to RAMAVAT Account from the Far6 Address. Then on September 30, the RAMAVAT Account received 20,000 USDT from the Far6 Address and sent 20,000 USDT to the RFaj Address. Based on the activity of September 28 through 30, I believe these transfers represents a cycle of laundering and obfuscation involving the same funds.

70. On October 1, 2022, the account only had one transaction, which was sending 19,996.8 USDT to an external Ethereum Blockchain Tether wallet. The balance of the RAMAVAT Account at this time, consisted of 5.50186 BTC and 12,510.25111 USDT.

71. On October 2, 2022, the RAMAVAT Account received 10,000 USDT from the rcRA Address. There was no other activity. The balance of the RAMAVAT Account at this time consisted of 5.50186 BTC and 22,510.25111 USDT.

72. On October 3, 2022, the RAMAVAT Account received 10,000 USDT from an external Tether Wallet belonging to the ByBit exchange. RAMATAV then conducted a series of trades involving bitcoin and Tether conversions in both directions on the P2P Marketplace resulting in the RAMAVAT Account's balance consisting of 5.64995 BTC and 29,623.82108 USDT.

73. I believe that the October 3 10,000 USDT deposit coupled with the October 2 10,000 USDT deposit, represents the return of laundered 19,996.8 USDT sent to an external wallet/exchange on October 1, 2022. I base this belief on my observances that the RAMAVAT Account, after converting the deposited bitcoin, would send specific amounts of Tether to alternating accounts at other exchanges. These same amounts would be deposited back into the RAMAVAT Account either as a whole amount or split between different exchanges within a day.

74. As part of my investigation, I was able to review some of the transactional records for accounts owned by other P2P exchanges which had either received Tether or sent Tether to the RAMAVAT Account. I was able to observe that all these accounts have a very high volume of USDT transfers into and immediately out of their accounts. Furthermore, after receiving USDT, all the accounts would rapidly transfer the same amount received out of their account to a wallet belonging to an account on a different exchange. I also noted that these accounts were conducting transfers with other accounts that had transferred Tether into or had received Tether from the RAMAVAT Account. I do not believe this was coincidental. I believe that these transactions occurring between the RAMAVAT Account and the other accounts are being conducted with the sole purpose of adding an additional layer of obfuscation and is part of the overall money laundering scheme being implemented by this organization.

75. There was no other activity observed in this account after this date and therefore I believe RAMAVAT could not access his account due to a freeze placed by OKX.

76. I have reason to believe that in addition to the bitcoin deposits of Victims 1-4, the other deposits into the VF8M Address represent proceeds from criminal activity which is part of a large-scale fraud scheme operating from India. Based on my observances, I believe that the bitcoin deposits into the VF8M Address are transactions that primarily originated from bitcoin kiosks in the United States and are more likely than not bitcoin defrauded from other unknown victims. Based on my use of blockchain forensic tools I know that that the larger deposits of Tether into the RAMAVAT Account originated directly and indirectly from other exchanges that offer Peer to Peer (P2P) trading services.

77. Based on my observations, my knowledge that the RAMAVAT Account received bitcoin from Victims 1–4, the sheer volume of transactions being conducted by the RAMAVAT Account as well as the monetary value represented by these transactions, I believed the RAMAVAT Account was involved in criminal activity and was being used to launder criminal proceeds. I also believed all the funds in the account represent proceeds of criminal activity and funds involved in money laundering.

78. On March 10, 2023, I applied to this Court and received authorization from the Honorable Judge Jeffrey Armistead to seize all cryptocurrency contained in the RAMAVAT Account (3:23-mc-00206).

79. As I mentioned earlier, the OKX exchange had placed a voluntary freeze on the RAMAVAT Account. This freeze was set to expire on March 13, 2023.

80. On March 10, 2023, I informed the OKX exchange that I had obtained a seizure warrant for the RAMAVAT Account and provided them a copy of the signed warrant in an effort to extend the freeze.

81. On March 14, 2023, OKX sent me an email asking HSI Portland to provide a cryptocurrency wallet address. I understood this to mean that OKX would voluntarily turn over the cryptocurrency in the RAMAVAT Account to HSI.

82. Beginning on March 29 and ending on March 30, 2023, the HSI Portland account received two transactions totaling 191,781.906863 USDT into HSI Portland's cryptocurrency exchange account. Although I did not receive any email informing that OKX was sending or had sent the cryptocurrency, I believe these transfers were a result of OKX exchange voluntarily turning over the funds subject to the federal warrant. I base this on the fact that at the time of

receipt of these funds, the value was consistent with the value of the cryptocurrency contained in the RAMAVAT Account that was frozen by OKX.

83. On April 7, 2023, I received a final correspondence from OKX, which was an email informing that on April 11, 2023, OKX would be lifting the freeze on the RAMAVAT Account.

84. On May 8, 2023, HSI converted the seized cryptocurrency received from OKX into fiat currency, which resulted in the receipt of $187,191.68.

**CONCLUSION**

85. Based on the foregoing information, I have probable cause to believe, and do believe, that the $187,191.68 in U.S. currency traceable to Shaishav RAMAVAT's OKCoin account is subject to seizure pursuant to 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C), as monies involved in transactions or attempted transactions or traceable to money laundering offenses in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1957 (unlawful monetary transactions in excess of $10,000), and is property constituting or derived from proceeds obtained, directly or indirectly, from a violation of 18 U.S.C. § 1343 (wire fraud).

I declare under penalty of perjury that the forgoing is true and correct pursuant to 28 U.S.C. § 1746.

Executed this 19th day of September 2023.

*s/ Guy Gino*
Guy Gino
Senior Special Agent
Homeland Security Investigations